UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/616,680	07/09/2003	John Apostolopoulos	200209975-1	2579

22879 7590 06/19/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

NOTIFICATION DATE	DELIVERY MODE
06/19/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/616,680	APOSTOLOPOULOS ET AL.	
	Examiner	Art Unit	
	BRANDON S. HOFFMAN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 13-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 13-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 and 13-44 are pending in this office action, claim 12 is canceled.

2. Applicant's arguments, file January 28, 2008,, have been considered and are persuasive. However, a new ground of rejection is made.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-5, 7, 8, 11, 13, 14, 16, 17, 19-22, 30, 36, 37, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhu et al. (U.S. Patent Pub. No. 2004/0196975) in view of Definition (Definition of Cryptographic Checksum, pulled from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci869866,00.html).

Regarding claim 1, Zhu et al. teaches a method of ensuring integrity of data, comprising:

- Separating an amount of data into segments **comprising a plurality of truncatable units** (paragraph 0043 and fig. 2, ref. num 102);

- Computing a cryptographic checksum for said segment (paragraph 0043, and MAC or Message Authentication Code); and
- Combining a segment and an associated cryptographic checksum into a data packet (paragraph 0045).

Zhu et al. does not specifically teach cryptographic checksums.

Definition teaches a message authentication code to be the same as a cryptographic checksum (page 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to interchange a cryptographic checksum and a message authentication code, as taught by Definition, with the method of Zhu et al. It would have been obvious for such modifications because the two terms are interchangeable to mean a hash function that is calculated on data to later be checked for integrity.

Regarding claim 2, Zhu et al. as modified by Definition teaches wherein said data comprises media data (see fig. 2, ref. num 102 of Zhu et al.).

Regarding claim 3, Zhu et al. as modified by Definition teaches wherein said data comprises secure scalably streamable data (see paragraph 0031 of Zhu et al.).

Regarding claim 4, Zhu et al. as modified by Definition teaches wherein said data is transmittable in a network (see paragraph 0004 of Zhu et al.).

Regarding claim 5, Zhu et al. as modified by Definition teaches wherein said data is stored in a storage medium (see paragraph 0009 of Zhu et al.).

Regarding claim 7, Zhu et al. as modified by Definition teaches further comprising forwarding said data packet (see fig. 3, ref. num 212 and 214 of Zhu et al.).

Regarding claim 8, Zhu et al. as modified by Definition teaches wherein said data to be streamed comprises a plurality of said data packets (see paragraph 0057 of Zhu et al.).

Regarding claim 11, Zhu et al. as modified by Definition teaches wherein said cryptographic checksum is computed for a truncatable unit in said segment (see paragraph 0043 of Zhu et al.).

Regarding claims 13 and 19, Zhu et al. as modified by Definition teaches wherein a cryptographic checksum is computed for each of said truncatable units in said segment (see paragraph 0043 of Zhu et al.).

Regarding claims 14 and 20, Zhu et al. as modified by Definition teaches wherein a first cryptographic checksum is calculated for a first truncatable unit, and wherein a second cryptographic checksum is calculated for the combination of a second truncatable unit, said first truncatable unit, and said first cryptographic checksum (see paragraph 0031 of Zhu et al.).

Regarding claim 16, Zhu et al. teaches a method for providing security to a scalably streamed media signal in a network, comprising:

- Separating said streaming media signal into a plurality of truncatable units (paragraph 0043 and fig. 2, ref. num 102);
- Computing a cryptographic checksum for each of said truncatable units (paragraph 0043, and MAC or Message Authentication Code);
- Appending said associated cryptographic checksum onto each of said truncatable units (paragraph 0043);
- Combining one or more of said truncatable units and associated cryptographic checksums into a transmittable data packet (paragraph 0045); and
- Forwarding said data packet (fig. 3, ref. num 212 and 214).

Zhu et al. does not specifically teach cryptographic checksums.

Definition teaches a message authentication code to be the same as a cryptographic checksum (page 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to interchange a cryptographic checksum and a message authentication code, as taught by Definition, with the method of Zhu et al. It would have been obvious for such modifications because the two terms are interchangeable to mean a hash function that is calculated on data to later be checked for integrity.

Regarding claim 21, Zhu et al. as modified by Definition teaches wherein the size of said truncatable units is selected to ensure the size of said data packet is transmittable in said network (see paragraph 0047 of Zhu et al.).

Regarding claim 22, Zhu et al. as modified by Definition teaches wherein said associated cryptographic checksum is computed independently for its associated truncatable unit (see paragraph 0043 of Zhu et al.).

Regarding claim 30, Zhu et al. teaches a computer readable medium having a data packet stored therein for causing a functional change in the operation of a device, said data packet comprising:

- A plurality of truncatable units, each of said units comprising an amount of media data (paragraph 0043); and
- A cryptographic checksum computed for each of said truncatable units (paragraph 0043, and MAC or Message Authentication Code).

Zhu et al. does not specifically teach cryptographic checksums.

Definition teaches a message authentication code to be the same as a cryptographic checksum (page 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to interchange a cryptographic checksum and a message authentication code, as taught by Definition, with the method of Zhu et al. It would have been obvious for such modifications because the two terms are interchangeable to mean a hash function that is calculated on data to later be checked for integrity.

Regarding claim 36, Zhu et al. as modified by Definition teaches wherein said cryptographic checksum is computed based on one truncatable unit (see paragraph 0043 of Zhu et al.).

Regarding claim 37, Zhu et al. as modified by Definition teaches wherein said cryptographic checksum is computed based on a plurality of truncatable units and associated checksums (see paragraph 0043 of Zhu et al.).

Regarding claim 44, Zhu et al. as modified by Definition teaches wherein each of said truncatable units is enabled to be deleted from said transmittable packet

independently of other truncatable units in said packet (see paragraph 0031 of Zhu et al.).

Claims 6, 9, 10, 15, 17, 18, 23-29, 31-35, and 38-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhu et al. (U.S. Patent Pub. No. 2003/0103571) in view of Definition (U.S. Patent Pub. No. 2004/0196975), and further in view of Chang et al. (U.S. Patent No. 6,963,972).

Regarding claims 6 and 17, Zhu et al. as modified by Definition teaches all the limitations of claim 1, above. However, Zhu et al. as modified by Definition does not teach further comprising applying a transcoder-readable header to said data packet.

Chang et al. teaches further comprising applying a transcoder-readable header to said data packet (col. 10, lines 54-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine further comprising applying a transcoder-readable header to said data packet, as taught by Chang et al., with the method of Zhu et al./Definition. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which allows changes in quality without having to decrypt the data.

Regarding claims 9 and 23, Zhu et al. as modified by Definition teaches all the limitations of claim 1, above. However, Zhu et al. as modified by Definition does not teach further comprising encrypting said segment and said cryptographic checksum.

Chang et al. teaches further comprising encrypting said segment and said cryptographic checksum (col. 4, lines 5-9).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encrypting the data, as taught by Chang et al., with the method of Zhu et al./Definition. It would have been obvious for such modifications because encryption secures sensitive data from unauthorized viewers.

Regarding claims 10, 18, and 27, Zhu et al. as modified by Definition/Chang et al. teaches wherein said packet is enabled to be decrypted independently of other packets comprising said streamed media data (see fig. 12 of Chang et al.).

Regarding claims 15, 24, and 38, Zhu et al. as modified by Definition teaches all the limitations of claim 1, above. However, Zhu et al. as modified by Definition does not teach wherein said cryptographic checksum is computed using a hash function.

Chang et al. teaches wherein said cryptographic checksum is computed using a hash function (col. 12, lines 19-35).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a hash, as taught by Chang et al., with the method of Zhu et al./Definition. It would have been obvious for such modifications because hashes provide tamper protection (see col. 12, lines 19-25 of Chang et al.).

Regarding claim 25, Zhu et al. as modified by Definition teaches further comprising accessing said data packet (see fig. 2, ref. num 102 of Zhu et al.) and forwarding said data packet (see fig. 2, ref. num 210 of Zhu et al.).

Zhu et al./Definition does not teach reading a transcoder-readable header of said data packet and deleting one or more of said truncatable units.

Chang et al. teaches reading a transcoder-readable header of said data packet (col. 10, lines 54-62) and deleting one or more of said truncatable units (col. 13, lines 28-43).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine deleting one or more of said truncatable units, as taught by Chang et al., with the method of Zhu et al./Definition. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which allows changes in quality without having to decrypt the data. Deleting units allows lower quality data to be transmitted to low-end devices.

Regarding claim 26, Zhu et al. as modified by Definition/Chang et al. teaches further comprising:

- Writing a new transcoder-readable header for said data packet reflecting said deleting and applying said new transcoder-readable header to said data packet (see col. 13, lines 36-43 of Chang et al.).

Regarding claim 28, Zhu et al. as modified by Definition/Chang et al. teaches wherein said deleting comprises transcoding said data packet (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 29, Zhu et al. as modified by Definition/Chang et al. teaches wherein said transcoder-readable header comprises information related to the content of said data packet while leaving said truncatable units undecrypted (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 31, Zhu et al. as modified by Definition teaches all the limitations of claim 30, above. However, Zhu et al. as modified by Definition does not teach wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums.

Chang et al. teaches wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums (col. 10, lines 54-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums, as taught by Chang et al., with the medium of Zhu et al./Definition. It would have been obvious for such modifications because the transcoder readable header enables transcoding, which allows changes in quality without having to decrypt the data.

Regarding claim 32, Zhu et al. as modified by Definition/Chang et al. teaches wherein said transcoder readable header enables transcoding said data packet (see col. 13, lines 28-43 of Chang et al.).

Regarding claim 33, Zhu et al. as modified by Definition/Chang et al. teaches wherein said truncatable units and said cryptographic checksums are enabled to be encrypted independently of said transcoder readable header (see fig. 12 of Chang et al.).

Regarding claim 34, Zhu et al. as modified by Definition/Chang et al. teaches wherein said truncatable units and said cryptographic checksums are enabled to be decrypted independently of said transcoder readable header (see fig. 12 of Chang et al.).

Regarding claim 35, Zhu et al. as modified by Definition/Chang et al. teaches wherein said transcoder readable header is enabled to be read independently of said truncatable units and said cryptographic checksums (see fig. 12 of Chang et al.).

Regarding claim 43, Zhu et al. as modified by Definition/Chang et al. teaches wherein said transcoder readable header is enabled to be written independently of said truncatable units and said cryptographic checksums (see fig. 12 of Chang et al.).

Regarding claims 39-42, Zhu et al. as modified by Definition teaches all the limitations of claim 30, above. However, Zhu et al. as modified by Definition does not teach wherein said cryptographic checksum is calculated using a message digest, message authentication code, keyed-hashing-for-message-authentication, and a digital signature function.

Chang et al. does not teach wherein said cryptographic checksum is calculated using a message digest, message authentication code, keyed-hashing-for-message-authentication, and a digital signature function (col. 9, lines 32-37).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine calculating the checksum using a variety of different functions, as taught by Chang et al., with the medium of Zhu et al./Definition. It would have been obvious for such modifications because hashes provide tamper protection (see col. 12, lines 19-25 of Chang et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S. HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2136